ABSTRACT

The cloning source of an authorized receiving device cannot be identified. A key distribution system 1 concerning the present invention includes: a communication channel 10; a key distribution center 11; a server 12; and receiving devices 13a to 13n. The key distribution center 11 distributes, to the server 12, the information necessary for distributing shared keys SK to the receiving devices 13a to 13n, and distributes the individual information group EMMG necessary for receiving the shared keys SK from the server 12. The server 12 generates the shared keys SK, generates the common information ECM based on the shared keys SK and the system secret variable group set SPGS, and distributes the common information ECM to the receiving devices 13a to 13n. The receiving devices 13a to 13n obtain the shared keys SK based on the individual information group EMMG and the common information ECM and outputs them to outside.